NLNETLABS

ANNUAL REPORT 2024

Table of Contents

About NLnet Labs

NLnet Labs is a not-for-profit foundation, founded in 1999. Over the past 25 years our mission has been to develop open-source software and open standards for the benefit of the internet, and to perform applied research on internet protocols. We focus our efforts specifically on the Domain Name System and inter-domain routing. NLnet Labs' work supports the robustness, security and reliability of the internet and safeguards the privacy of its users.

You may not have heard of us. But if your email arrived, your government site loaded, or your cloud platform didn't blink—you've probably already met us.

Hospitals. Borders. Banks. The big brands you love. Entire countries. Our code runs there.

You'll find us under the hood of national domains, global platforms, and backbone networks—doing quiet work that matters. We don't chase the spotlight. We keep it on—for everyone else.

We're a nonprofit. Since 1999, we've built DNS and routing software that holds up under pressure. No licenses to unlock. No "enterprise edition." Everything we make is open-source, production-grade, and backed by a team of experts who show up when it counts.

But we don't just write code. We help write the rules. You'll find us in IETF working groups, shaping the open standards and protocols the internet runs on—because infrastructure needs more than software. It needs stewardship.

We believe the systems we all depend on should be open, resilient, and supported by code-enthusiasts who know their stuff. That's the work. That's the mission. That's us.

Mission

NLnet Labs, established in 1999 as a nonprofit foundation, develops open-source software and publicly accessible standards designed to enhance the Internet. Open-source software allows anyone to review, modify, and improve the source code, while open standards are freely accessible guidelines created through open processes. We also actively collaborate with other developers to promote interoperability among implementations, encouraging widespread adoption of open standards. Our goal is to ensure a robust, secure, and reliable Internet while protecting user privacy.

To achieve our mission, we collaborate with key Internet organisations globally. Our peers recognise us as influential contributors in developing and advocating open standards and open-source software. We are widely regarded as leading experts in fundamental Internet technologies, particularly DNS and routing. Our collaborations include work with organisations

such as the Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs), the Internet Corporation for Assigned Names and Numbers (ICANN), prominent Top Level Domain (TLD) operators, associations like CENTR, and networking communities including RIPE, OARC, NANOG, as well as individual researchers and major industry stakeholders.

Organisation

We are a lean organisation with a team of around 16 people, consisting almost exclusively of developers and researchers, with minimal overhead. We attract talented people who want to make a difference to the well-being of the internet, with a profound belief in open source and open standards.

We develop open-source software widely adopted throughout the Internet industry, from DNS root servers at the heart of the Internet to compact, embedded devices running secure recursive resolvers. Additionally, we create routing software designed to secure large operators' networks and enhance network observability and manageability.

Our researchers pioneer new technologies, help define future standards, and build prototypes of technologies that promise to improve the internet. We increase understanding of the internet by studying its fundamental building blocks. By actively participating in both worlds — development and research — we bridge the gap between academia and industry, and introduce solutions that are practical as well as innovative.

We also contribute to policy and governance by bridging technology and policy. Our technical expertise and advice is widely recognised by policy-making bodies. We advise on public policy decisions that affect the security and privacy of internet users across the globe, as well as the stability of the internet itself.

Our strategic goals

Our aim is to deliver solutions that strengthen trust, security, privacy, scalability, and the global nature of the Internet. To support this, we actively engage in research and innovation focused on DNS and routing technologies.

DNS

NLnet Labs is widely recognised for developing the authoritative DNS name server NSD and the recursive, validating DNS resolver Unbound. By introducing robust open-source alternatives, we have strengthened the stability and resilience of the Internet and accelerated the adoption of DNSSEC.

We have also advanced DNS security and privacy at the user level through tools like dnssec-trigger and libraries like getdns, which bring protection directly to the end-user. These projects have influenced broader development efforts: dnssec-trigger concepts, for example, have been adopted by Gnome NetworkManager, while insights from getdns continue to inform our ongoing and upcoming work, as outlined in the following sections.

We remain committed to providing a stable and secure DNS, which supports broader Internet trust and security while safeguarding user privacy. Looking ahead, we are focusing on three key areas: improving DNS libraries and APIs for developers; enhancing modularity and ease of integration for DNS operators; and scaling up the size and performance of our solutions.

Routing

Our work in routing focuses on two main goals: (i) strengthening BGP routing by leveraging RPKI for greater robustness and future security, and (ii) giving network operators better visibility into BGP data to help them enhance the stability and quality of their infrastructure.

Currently, RPKI is primarily used for Route Origin Validation (ROV) to help prevent accidental route misoriginations. We maintain the widely used Krill RPKI Certificate Authority (CA) suite, which is used by an RIR, several National Internet Registries (NIRs) and over 2,000 member organisations. In terms of validation, our Routinator tool is the most widely used RPKI validator suite, helping operators to filter routes with invalid origins.

We developed the Rotonda toolset to improve observability and manageability in inter-domain routing. Rotonda can collect and analyse BGP and BMP (BGP Monitoring Protocol) data from routers and provides operators with programmable components for monitoring and managing their BGP workflows. The toolset allows other data sources, such as RPKI, to be integrated into routing filtering, selection and management. Stand-alone applications such as route servers or looking glasses can also be built using Rotonda.

Community

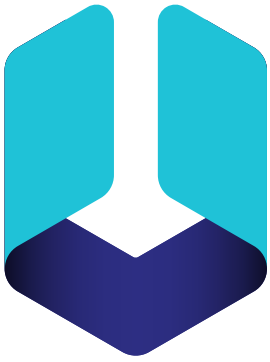
Over the past two and a half decades, NLnet Labs has worked carefully on its visibility and reputation as an expert on DNS and inter-domain routing. Our active involvement in the standardisation community at IETF and operations communities such as RIPE, CENTR and OARC has established us as an organisation possessing extensive knowledge of the Internet's functioning and its foundational elements.

Beyond technical contributions, we actively provided expertise to the policy-making community through participation in the ICANN community and national governmental advisory committees on open standards. With the growing involvement of governments with internet governance, the regulation of internet operators and software itself, we are uniquely positioned to make meaningful contributions to these discussions. A recent example is our contribution to policy discussions in the EU about regulating software based on our decades of experience with open source software.

DNS activities and results

We have continued to develop and improve our prime products, NSD and Unbound, which are used at virtually every level of the internet by everyone from individuals to the largest network operators, content delivery networks (CDNs) and cloud providers. We are at the forefront of developing new standards and incorporating them into our software. We are also in dialogue with the industry to ensure that we can cater for their needs when it comes to offering services to their customers.

Our strategy is not to rewrite our existing products that currently power much of today's DNS infrastructure in the world but to rethink how people develop and deploy software that uses the domain name system. Over the next few years, NLnet Labs aims to provide a full-featured DNS library using the Rust programming language. This library will enable developers to create software that meets the demands of the modern internet, from applications on compact embedded devices to large-scale server farms. Adopting our library is expected to facilitate the seamless integration of name services with applications and services, encouraging the use of secure and private defaults. Just as Let's Encrypt achieved worldwide adoption of TLS, we want to promote secure name resolution.



We started the development of 'domain', our DNS library in Rust, in 2018 as a Friday-afternoon project. From 2024 year onwards, the project got a dedicated team of developers and the organisation's long-term commitment. In light of this goal, we received a grant from Sovereign Tech Fund to expand the 'domain' library with essential functionality.

The 'domain' library aims to provide a comprehensive – ideally complete – range of building blocks necessary to build specialised DNS applications or include uses of DNS in other applications. By now, it provides several foundational features centred around representing the components of a DNS message – domain names, resource records, etc. – and creating, parsing, and processing them. In addition, it contains a simple, async stub resolver that you can use to initiate specific queries towards upstream resolvers. Throughout 2024, we have extended the foundation to cover most functionality necessary to build other DNS components: authoritative servers, simple resolvers, and proxies.

Our goal is to enable operators to integrate their business logic and traffic engineering requirements directly into DNS infrastructure, while also removing barriers to DNSSEC adoption by providing a flexible and accessible signing solution.

One of NLnet Labs' key goals in the coming years is to develop a new DNSSEC signing solution. This solution will support multiple backend storage formats and provide flexible options for provisioning and management.

Together, these efforts aim to modernise authoritative DNS services and make advanced functionality more accessible to a broader range of users.

For the client side of 'domain', we added response caching and DNSSEC validation. On the server side, we provided means to load zones from zone files, keep them available in memory, and use them to answer queries. We also offered the means for zone transfers, both its primary and secondary sides. Finally, DNSSEC signing of zones and key management round out the server functionality.

Because the only way to judge the quality of these components is to use them in a real-world scenario (and because this is something that many people have asked for), we started work on a flexible DNS proxy which allows you to define rules for how to handle requests – whether to have them answered by a specific upstream server, from a configured local zone, or even not at all – based on properties of the request.

We believe a fresh implementation of a DNS diagnostics tool will be valuable to the DNS community. The idea is to provide functions beyond simple DNS queries. For instance, it could allow you to check the DNSSEC status of a zone or whether your local resolver provides answers that match those given by the authoritative servers. We offered all of this functionality in an initial version of our DNS inspection toolset 'dnsi'.

Our ldns C library includes a number of tools for zone management – sign a zone, check the correctness of a zone, and so on. These were originally intended merely as examples for the library but have since been adopted for production purposes. In 2024, we released the first version of dnst, a Rust-based DNS toolbox that provides drop-in replacements for the most commonly used ldns example programs.

Routing activities and results

Krill and Routinator are continually being developed to incorporate new standards and features based on industry needs. For example, we recently added TAL management to Krill for LACNIC, enabling them to start migrating their RPKI CA infrastructure to it.

To strengthen and expand our software portfolio, NLnet Labs aims to play a leading role in developing software that supports inter-domain routing. Our goal is to enhance the quality and security of the global routing system by building on our existing tools, Krill and Routinator, and introducing a new modular, analytical BGP engine: Rotonda.

Rotonda is a flexible tool that allows users to create custom BGP routing applications by combining programmable components. Its architecture supports real-time reprogramming and

reconfiguration, offering high adaptability. Although designed for inter-domain routing, Rotonda is equally valuable for individual networks, enabling operators to build tailored monitoring and management tools. Its versatility and scalability make it well-suited to address key challenges such as security, visibility, and operational reliability.

As part of its development, we are creating a scalable data store with advanced search and query capabilities. This will provide network operators and Internet Exchange Points (IXPs) with detailed, real-time views of the inter-domain routing landscape, strengthening the Internet's overall resilience and security.

Thanks to its modular design, Rotonda can power a broad range of applications for network operators and IXPs. These include looking glasses, route reflectors, route servers, and full-featured BGP routers—all built to scale efficiently, regardless of routing volume or session complexity.

One of the most important developments in 2024 is the introduction of an embedded scripting language for Rust, called Roto. This language aims to be a simple, yet fast and reliable scripting language for Rust applications. The need for Roto comes from Rotonda. Mature BGP applications usually feature some way to filter incoming route announcements. The complexity of these filters often exceed the capabilities of configuration languages. With Rotonda, we want to allow our users to write more complex filters with ease. So we decided to give them the power of a full scripting language.

We have some hard requirements for this language. First, we need these filters to be fast. Second, Rotonda is critical infrastructure and so runtime crashes are unacceptable. This rules out dynamically typed languages, of which there are plenty in the Rust community. We want a statically typed language which can give us more type safety and speed. Finally, we want a language that is easy to pick up; it should feel like a statically typed version of scripting languages you're used to.

Roto fills this niche for us. In short, it's a statically typed, JIT compiled, hot-reloadable, embedded scripting language. To get good performance, Roto scripts are compiled to machine code at runtime.

Community activities and results

Technical community and standards

Over the past two and a half decades, NLnet Labs has carefully built its visibility and reputation as a leading expert in DNS and inter-domain routing. Our active participation in standardisation efforts at the IETF, and in operational communities like RIPE, CENTR, and OARC, has established us as a trusted authority on the Internet's core infrastructure.

Our involvement in the IETF aligns with our core objectives of ensuring the Internet's security, privacy, and stability. Ongoing discussions with industry partners regarding operational challenges and the delivery of practical solutions share our activities within those principles. NLnet Labs has actively contributed to and co-authored numerous Internet Drafts (I-Ds) and

RFCs, initially focusing on DNS and expanding into RPKI and inter-domain routing. Developing IETF standards places a significant emphasis on proof-of-concept implementations and interoperability, collectively called running code. By providing early implementations of (draft) standards, we actively contribute to the evolution of open standards within the IETF.

Another significant activity involves applied research to develop and evaluate new technologies, study operational challenges, and validate solutions. Historically, we have undertaken research projects in collaboration with or on behalf of various organisations, including NLnet, SURF, ICANN, ISOC, and RIPE NCC, as well as with companies such as Verisign and Comcast. The outcomes of these applied research projects have consistently earned high regard within the community, contributing to industry advancements. This impact is evident through deeper operational insights leading to improved operational practices (BCOPs – best current operational practices) and enhancements to standards and implementations. Our enduring relationships with these organisations often lead to invitations for project participation or research project tenders.

In 2024, we contributed:

- RSSAC047 in Focus: A closer look at reachability and publication delay: In collaboration with SIDN, we contributed to the report on validating the availability and publication delay measurements of the initial implementation of the RSSAC047 measurement software, which ICANN developed to assess root server system performance as defined in RSSAC047v2. Our analysis shows that while the software generally works as intended, many reported availability issues likely originated from the measurement vantage points or network paths rather than the root servers themselves.
- The reduced risk of redirected query traffic with signed root name server data: In this study, we evaluate the potential security benefits of DNSSEC signing the root-servers.net zone, which currently provides unsigned authoritative data for the root server identifiers. Our analysis shows that while signing this zone would reduce the risk of redirected query traffic—where attackers spoof root server addresses—the overall reduction is modest, estimated at about 1.2% based on 2023 DITL data. We recommend that resolvers obtain root server addresses authoritatively, as this already lowers the risk of redirection and, when combined with DNSSEC-signed root data, fully mitigates on-path attack scenarios.

Bridging Technology & Policy

Beyond technical work, we contribute to policy discussions through engagement with the ICANN community and national governmental advisory committees, offering insights grounded in our long-standing experience with open standards and open-source software. As governments become increasingly involved in Internet governance and regulation, extending even to software itself, our role becomes ever more vital. A recent example is our contribution to EU policy discussions on software regulation. Embedding our expertise across standardisation, operational, and policy-making communities not only supports our strategic goals but also ensures our continued relevance and sustainability.

This engagement enhances our visibility, promotes adoption of our solutions, drives collaborative research, bridges gaps between engineers and policymakers, and helps secure development partnerships and support contracts.

In 2024, we contributed:

- An "Open Source In The European Legislative Landscape devroom" at FOSDEM 2024, co-organised with the Open Source Initiative, Free Software Foundation Europe, Eclipse Foundation, Open Forum Europe and the European Commission. This devroom was a first and brought together EU policymakers and FOSS developers for a day long discussion on the interaction of software regulation (CRA), strict liability (PLD), platform regulation (DMA) and other EU regulatory activity for the work of the FOSS community.
- Feedback, resulting in changes to the NIS2 implementing act for the digital sector, in particular with respect to supply chain security requirements for the developers of Free and Open Source Software and its use by operators of essential services in Europe, such as DNS operators and TLD registries. On the same topic, we contributed to ENISA's drafting of guidance for this act, with results expected to be published in 2025.
- Co-chairing research into the use of Free and Open Source Software in global domain name registration and DNS infrastructure in ICANN's Security and Stability Advisory Committee (SSAC), for a 2025 publication with a target audience of policymakers and regulators.

Report of the Supervisory Board

The Supervisory Board oversees the policy of the Management Board and the general affairs of Stichting NLnet Labs. In addition to its supervisory responsibilities, the Board acts as a strategic sparring partner. In 2024, the main areas of attention were strategy, financial sustainability, and governance.

Year in Brief

The Supervisory Board met four times with the Management Board. It approved the 2023 financial statements and annual report, as well as the annual plan and budget for 2025. The Board also conducted its annual self-evaluation to reflect on its own performance and effectiveness.

Key Themes

Growth and Strategy

A core objective in 2024 was to strengthen the long-term sustainability of the foundation by increasing revenue from support contracts and sponsored feature development. These activities are carried out through Open Netlabs B.V., the wholly owned subsidiary that handles commercial services in support of the foundation's public-benefit mission. In 2025, the Board will pay particular attention to how the strategic choices made in 2024 translate into measurable commercial results and a durable business model.

Finance and Risk

With financial sustainability as a key priority, the Supervisory Board asked for greater transparency and predictability through timely figures, scenarios, and clear KPIs. The 2024 financial results were positive, supported in part by subsidies. However, continued reliance on

subsidies remains a point of attention. Diversification of revenue and further development of the financial model will therefore be important themes for 2025.

Governance and Compliance

The Supervisory Board and Management Board updated their respective regulations to clarify powers, reporting lines, and confidentiality arrangements. The Board also decided to include its own annual reflection as part of the published report. On compliance, the Board was informed about the implications of the EU Cyber Resilience Act and the strategic decisions required in the coming years. The compliance strategy will be further developed in 2025.

Composition

As of 31 December 2024, the Supervisory Board consisted of five independent members, with terms of office and roles defined in the Board's regulations. The Board included some overlap in terms with newly appointed members to ensure continuity.

NLnet Labs Supervisory Board in 2024		
Name	**Role**	**End of Term**
Cristian Hesselman	Chair	30 June 2024
Bart Nieuwenhuis	Chair	1 July 2027
Marieke Huisman	Secretary	1 January 2027
Andrei Robachevsky	Member	1 January 2027
Jochem de Ruig	Treasurer	31 December 2024
Loek Bakker	Member	1 January 2027
Niels Westerlaken	Member	1 January 2027

Financial Report

Income From Support and Development

A key objective in 2024 was to further increase revenue from support contracts and sponsored feature development. These activities are carried out through Open Netlabs B.V., the wholly owned and taxable subsidiary of NLnet Labs, which operates in line with the foundation's public-benefit mission and governance framework.

Open Netlabs offers support contracts for our production-grade software, including NSD, Unbound, Krill and Routinator. These contracts provide customers with service-level support, early access to security patches, and an opportunity to contribute financially to our open-source mission. In addition, it provides training, software development on internet security standards, and consulting services such as installation support, optimisation, and audits.

Grants and Subsidies

Since 2012, NLnet Labs has received substantial annual support from SIDN, renewed in 2022 for another five years. We are also grateful for the long-term grants from Infoblox, Verisign, Meta, Comcast, and SUNET, as well as the many ad-hoc donations from organisations and individuals.

In-kind contributions were again vital in 2024: e.g. DigitalOcean, Fastly, Hertzner, and Amazon Web Services provided free services that enabled automated testing, analysis tooling, and a resilient production platform.

Income			
	2023 Actual (k€)	**2024 Actual (k€)**	**2024 Budget (k€)**
SIDN Subsidy	125	125	125
Other donations	162	271	230
Consultancy and other income	132	382	141
Research and projects	375	971	390
Income from Interest	3	4	1
Total	**797**	**1753**	**887**

Expenditure			
	2023 Actual (k€)	**2024 Actual (k€)**	**2024 Budget (k€)**
Staff	693	682	690
Housing	73	72	74
Travel	31	37	35
Depreciation	5	3	0
Project Costs	75	591	0
Other Costs	45	41	35
Sub Total	922	1426	834
Negative Result Open Netlabs B.V.	144	-154	0
Project Reservations	-269	481	53
Total	**797**	**1753**	**887**

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	2	General Reserve	1388
Open Netlabs B.V. Stock and Loans	237	Special Purpose Reserves	200
Receivables	385	Current Liabilities and Accruals	261
Bank and Cash	1225		
Total	**1849**		**1849**

Looking Ahead

In the coming year, we expect our new projects to mature further and attract interest from users in academia, industry, and the wider technical community. The progress on the Domain DNS library offers opportunities to build new DNS applications and services in Rust that strengthen the DNS ecosystem. These developments are also expected to support industry adoption and contribute to long-term financial sustainability.

Rotonda has already generated substantial attention within the routing community, both in research and operational settings. In 2025, our focus will be on concrete use cases that demonstrate the framework's practical value and help establish a sustainable funding model for its continued development. Meanwhile, NSD, Unbound, and Routinator remain products with strong demand for support contracts.

Overall, we are actively exploring new opportunities to apply our research and software development results in innovative solutions and services that benefit academic users, industry partners and individuals.

Our team has remained stable for several years, and we do not foresee additional growth in full-time equivalents in the coming years. The current team size is expected to be sufficient to achieve our strategic objectives.

Colophon

Photo Credits

Photo on page 7 by Brett Garwood on Unsplash

Contact

Stichting NLnet Labs
Science Park 400
1098 XH Amsterdam
labs@nlnetlabs.nl
www.nlnetlabs.nl

© NLnet Labs